REMARKS

Applicant respectfully requests reconsideration of the present application in view of the foregoing amendments and in view of the reasons that follow. At the time of the outstanding Office Action, claims 1, 3-8, 10-15, 17-21 and 23-32 were pending. A detailed listing of all claims that are, or were, in the application, irrespective of whether the claim(s) remain under examination in the application, is presented, with an appropriate defined status identifier.

Prior Art Rejection:

In the Office Action, claims 1, 3-8, 10-15, 17-21 and 23-32 were rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 6,175,917 to Arrow et al. (hereinafter "Arrow") in view of U.S. Patent Application Publication 2001/0042201 to Yamaguchi et al. (hereinafter " Yamaguchi"). Applicant respectfully traverses this rejection for at least the following reasons.

The instant invention deals with managing IPSec sessions in an IPSec setting server, such that authentication and security parameter setting occurs on a server rather than remote machines utilizing the network security protocol. Correspondingly, claim 1 recites a network comprising "an IPsec setting server apparatus, which manages IPsec settings of said IPsec processing apparatuses, wherein said IPsec setting server apparatus includes means for **collectively managing policies of said IPsec to be applied between first and second IPsec processing apparatuses**, and wherein **said IPsec setting server apparatus includes means for specifying policies of said IPsec to be applied between said first and second IPsec processing apparatuses based upon contents of a request message for communication between said first and second IPsec processing apparatuses** received from said first IPsec processing apparatus." (emphasis added) Claims 8, 15 and 21 recite analogous features.

Arrow teaches a Virtual Private Network (VPN) that includes a VPN management station 160 and VPN units 115, 125, 135, and so on, under the control of the VPN management station. The Examiner asserts that the VPN management station 160 of Arrow allegedly teaches the feature of an IPsec setting server apparatus. The VPN management station controls the VPN

units through commands and configuration information transmitted to each VPN unit. The Examiner asserts that the VPN units teach the feature of IPSec processing apparatuses.

Applicants note that the independent claims utilize an IPSec setting server apparatus and IPSec processing apparatuses. The Examiner correctly indicates that Arrow fails to teach IPSec, and also recognizes a difference between a VPN and a VPN utilizing IPSec.

The VPN management station configures each individual VPN unit. There is no teaching or suggestion in Arrow that the VPN units have policies that are to be applied between them. Rather, the VPN management station applies configuration information to each individual VPN unit. The Examiner has pointed to Figures 1 and 13, and the corresponding text in the disclosure to teach that the "IPsec setting server apparatus includes means for collectively managing policies of said IPsec to be applied between first and second IPsec processing apparatuses." However, Figure 13 teaches a flow chart to show how a VPN system manager creates a single VPN unit. There is no teaching or suggestion in this Figure, or in Figure 1, of managing IPSec policies, or any policies for that matter, that are to be applied between two VPN units. Figure 13, and its corresponding text, depicts how to configure a single VPN unit for communication, with no mention of applying policies or setting configuration between more than one VPN unit. Thus, Applicants respectfully submit that Arrow has failed to teach this feature of the invention as claimed.

Similarly, the Examiner relies on configuration requests issued by the VPN management station 160, to configure a VPN unit. After receiving this configuration request, the VPN management station configures a VPN unit. Figure 6 details configuration data used to operate a VPN unit. There is no teaching or suggestion in Figure 6, or anywhere else in the disclosure of Arrow, that the configuration data includes information regarding applying policies between VPN units. Further, there is no teaching or suggestion in Arrow that receiving a configuration request leads the VPN management station to specify policies to apply between two VPN units, based upon the configuration request. Rather, as mentioned above, the configuration request is utilized to configure only one VPN unit. Applicants respectfully submit that there is no teaching

or disclosure in Arrow that "said IPsec setting server apparatus includes means for specifying policies of said IPsec to be applied between said first and second IPsec processing apparatuses based upon contents of a request message for communication between said first and second IPsec processing apparatuses received from said first IPsec processing apparatus."

Yamaguchi fails to make up for the deficiencies of Arrow as shown above. In Yamaguchi, an IKE (Internet Key Exchange) protocol is utilized in order to generate an encryption key (paragraph 0148). On the contrary, in our invention, since the IKE is not used for acquisition of the encryption key, it is not necessary to perform an arithmetic operation of Diffie-Hellman used in the IKE. Therefore, it become possible to reduce a time until the start of the IPsec processing compared to Yamaguchi (page 11, lines 18-24 of the specification).

Yamaguchi also fails to teach a network "wherein said IPsec setting server apparatus includes means for specifying policies of said IPsec to be applied between said first and second IPsec processing apparatuses based upon contents of a request message for communication between said first and second IPsec processing apparatuses received from said first IPsec processing apparatus." Yamaguchi states each apparatus maintains its own SA and SPDs (paragraph 0077). There is no teaching that there is a IPsec setting server that maintains these values, let alone an IPsec setting server apparatus that specifies IPsec policies to be applied between the apparatuses. Thus, even if the teachings of Yamaguchi were combined with those of Arrow, the features of the instant invention (an IPsec setting server apparatus with means for specifying policies) would be lacking.

If this rejection is maintained, the examiner is respectfully requested to point out where this feature is disclosed in either Arrow or Yamaguchi.

The dependent claims are also patentable for at least the same reasons as the independent claims on which they ultimately depend. In addition, they recite additional patentable features when considered as a whole.

Conclusion:

Applicant believes that the present application is now in condition for allowance. Favorable reconsideration of the application as amended is respectfully requested.

The Examiner is invited to contact the undersigned by telephone if it is felt that a telephone interview would advance the prosecution of the present application.

The Commissioner is hereby authorized to charge any additional fees which may be required regarding this application under 37 C.F.R. §§ 1.16-1.17, or credit any overpayment, to Deposit Account No. 19-0741. Should no proper payment be enclosed herewith, as by a check or credit card payment form being in the wrong amount, unsigned, post-dated, otherwise improper or informal or even entirely missing, the Commissioner is authorized to charge the unpaid amount to Deposit Account No. 19-0741. If any extensions of time are needed for timely acceptance of papers submitted herewith, Applicant hereby petitions for such extension under 37 C.F.R. §1.136 and authorizes payment of any such extensions fees to Deposit Account No. 19-0741.

Respectfully submitted,

Date May 22, 2008

By _____

FOLEY & LARDNER LLP
Customer Number: 22428
Telephone: (202) 945-6014
Facsimile: (202) 672-5399

George C. Beck
Attorney for Applicant
Registration No. 38,072

Ramya Ananthanarayanan
Agent for Applicant
Registration No. 59,597